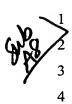
WHAT IS CLAIMED IS:



5

6 7

1 2

#

2

3

4

5

6

7

8

9

1011

1

2

- 1. A method of authenticating a client to a server comprising:
 generating a challenge at the client;
 signing the challenge to form a signed challenge;
 sending at least the signed challenge to the server;
 verifying the signature of the challenge at the server; and
 if the signature is verified, sending an indication of successful authentication to the
 client.
- 2. The method of claim 1, wherein generating a challenge at the client comprises generating a random number.
- 3. The method of claim 1, wherein generating a challenge at the client comprises generating a sequential challenge.
- 4. The method of claim 1, wherein generating a challenge at the client comprises generating a challenge based on data received from the server in a prior step.
- 5. The method of claim 4, wherein the data received from the server is a challenge returned with a server response to a prior client query.
- 6. A method of using a one time use card number for an online transaction, comprising:

generating a one-time use card number at a user system;

authenticating the user system to an issuer system;

passing the one-time use card number from the user system to the issuer system;

passing the one-time use card number from the user system to a merchant system,

wherein the merchant system is programmed to present the one-time use card

number to the issuer system to effect a payment;

verifying the one-time use card number received from the merchant system with the one-

time use card number received from the user system; and

if the one-time use card number is verified, approving the transaction.

7. The method of claim 6, wherein passing the one-time use card number to the issuer includes passing at least one other data element related to the online transaction.

- 8. The method of claim 7, wherein the at least one other data element is
- 2 selected from, or a function of, a user's account number, a user's private key, a transaction
- 3 time, a transaction amount, or a merchant ID.